



ELECTRONIC BANKING FRAUD IN SOUTH AFRICA: KEY DRIVERS IN THE DIGITAL AGE. A QUALITATIVE ANALYSIS

Tawona Matrokisi Chindara¹, Ebenezer Esenogho²

^{1), 2)} University of South Africa, Pretoria, South Africa

e-mails: ¹ chindtm@unisa.ac.za, ² esenoe@unisa.ac.za

Received: Feb 13, 2026

Accepted: April 13, 2026

Online Published: November 1, 2026

ABSTRACT

As South African banks rapidly adopt digital technologies, cybercriminals are exploiting system vulnerabilities with increasingly sophisticated tools, leading to a surge in e-banking fraud. This has resulted in financial losses, reputational damage, and heightened risks to ethical conduct and financial reporting. In response, banks are actively seeking effective defences to protect themselves and their clients from cyberfraud. However, to achieve this overarching aim, it is crucial to understand the underlying drivers of cybercrime and to adopt emerging technologies that uphold financial accountability. The objective of this study was to qualitatively identify the principal drivers of e-banking fraud prevalent within the South African financial system. A qualitative research design was employed, guided by the fraud diamond theory. Semi-structured interviews were selected as the most effective method of data collection, involving 15 purposively chosen senior risk officers from local banks and branches of international banks operating in South Africa. Data analysis was conducted using MAXQDA 24, through which key themes were identified to determine the drivers of e-banking fraud in the South African banking sector. The study found that weak judicial processes, poor internal controls, limited oversight, inadequate investment in new technologies, and low levels of fraud awareness are the primary drivers of e-banking fraud in South Africa. Furthermore, the study highlighted the potential of strategically adopting machine learning for real-time fraud detection, alongside stronger governance, judicial transparency, and sector-wide collaboration. In conclusion, the study recommends that the South African banking sector must urgently address these pressing challenges through the proposed practical measures, thereby enhancing resilience and safeguarding the nation's banking infrastructure, financial stability, reliable financial reports, and client trust in the digital age.

Keywords: South Africa, Electronic banking fraud, South African banking sector, Cybercrime, Machine Learning and Accountability, Integrity of Financial Reports.

JEL classification: O3, O31, O32, O33, M41

Paper type: Research article

Citation: Chindara, T.M., Esenogho, E. (2027). Electronic banking fraud in South Africa: key drivers in the digital age. A qualitative analysis. Access to science, business, innovation in the digital economy, ACCESS Press, 8(1), 9-28. [https://doi.org/10.46656/access.2027.8.1\(1\)](https://doi.org/10.46656/access.2027.8.1(1))

INTRODUCTION

The South African banking sector is hybrid in nature, comprising both local institutions and branches of international banks operating within the economy. Over the past decades, the widespread adoption of digital banking facilities has significantly transformed customer preferences (Tsai & Su, 2021). These shifts have placed growing pressure on banks to innovate to meet escalating client demands, the desire to access banking services around the clock and to perform transactions from the comfort of their homes or other convenient locations (Tsai & Su, 2021). In 2017, the South African Reserve Bank (SARB) made a landmark move in support of the digitisation of the banking sector by issuing licenses to three banks that operate fully digitally



(Dube, 2018). This move intensified competition among banks for attracting and retaining clientele, compelling many traditional institutions to adopt advanced technological tools in the provision of banking services (Nel & Boshoff, 2021).

Moreover, the outbreak of the COVID-19 pandemic and the resulting strict lockdowns aimed at curbing the virus further accelerated the demand for contactless banking solutions (South African Banking Risk and Information Centre (SABRIC), 2021; Laxman et al., 2024). On the positive side, Nel and Boshoff (2021) highlighted that the adoption of these technologies has yielded notable benefits for the global banking sector, enabling banks to serve clients more conveniently. However, the adoption of these advanced digital banking systems also carries significant risks (Tawde et al., 2024; Basel Committee on Banking Supervision, 2024). They expose banks to the escalating threat of e-banking, as cybercriminals exploit the capabilities of these technologies to craft complex and harmful fraudulent schemes that are difficult to detect and neutralise (Chindara et al., 2025a). Consequently, banks find themselves in a challenging dilemma and are urgently seeking robust solutions to shield themselves from these cyber threats (Malinka et al., 2022). This is supported by a study conducted by Silva and Dias (2023), which found that customers prioritise the security of their financial resources over other considerations. It is imperative that banks reinforce their security frameworks by advancing fraud mitigation systems to protect institutional reputation and maintain client confidence.

Bank fraud has been bedevilling financial institutions for centuries, and it was exacerbated by the rapid growth of the internet and the adoption of various digital banking services such as Automated Teller Machines (ATMs), debit and credit cards, and online banking platforms (Lee, 2025). Existing literature echoes this concern, emphasising that e-banking fraud represents a global challenge defined by both its scale and scope, while simultaneously undermining the soundness and stability of the financial system (Gupta et al., 2023; Basel, 2024). Laxman et al. (2024) likewise affirm that e-banking fraud constitutes one of the most pervasive risks confronting the banking sector and has escalated into a worldwide burden. Consistently, the LexisNexis Risk Solutions (2022) report revealed that, on average, digital banking fraud surged by 37% across high-performing markets, including Latin America, Europe/Middle East/Africa, and Asia-Pacific between 2021 and 2022. In India alone, Shetty (2024) reported a daily average of 800 reported cases of e-banking fraud. In South Africa, cybercriminals capitalising on generative Artificial Intelligence (AI) capabilities led to an estimated R3.3 billion in financial losses in 2023 alone (SABRIC, 2024). A year-on-year comparison between 2022 and 2023 revealed a significant surge in cybercrime, with digital banking fraud rising by 45% and other related financial crimes increasing by 47% (SABRIC, 2024). Notably, banking application fraud accounted for 60% of reported digital banking fraud in 2023, underscoring its severity (Mthimkhulu, 2024). Its prevalence rose by approximately 89% compared to the previous year (SABRIC, 2024).

These statistics reflect a pressing challenge in South Africa's banking sector and signal the need for urgent intervention to safeguard banks and their clients. In contrast, to enhance the desired security, South African banks have implemented a number of fraud mitigation tools such as multifactor authentication, blockchain technology, adoption of AI and machine learning (ML) algorithms, one-time PINs, security questions for login,



and biometric verification (Chindara, 2024). Despite these measures offering considerable security enhancements for banking institutions and clients, reports of fraud in the South African banking sector continue to rise (Pillay et al., 2023; SABRIC, 2021). While Sijan et al. (2022) attributed numerous adverse occurrences within e-banking platforms to systemic deficiencies, the persistent rise in reported e-banking fraud suggests an underlying issue. This has prompted researchers to investigate the actual drivers of e-banking fraud through qualitative inquiry, aiming to gather detailed insights from respondents. This aligns with Ramamoorti (2008), who emphasised the importance of business leaders and management understanding the root causes of fraud, the individuals who commit it, and the key motivators behind it, to develop proactive measures for its mitigation. Therefore, the current study seeks to explore the primary drivers behind the occurrence of e-banking fraud within the South African banking industry, with the aim of informing both management and policymakers on the appropriate measures that need to be enacted to effectively mitigate the fraud epidemic. The remainder of the article is organised into the following sections: literature review, research methodology, presentation and discussion of results, research implications and recommendations, and finally, the conclusions.

LITERATURE REVIEW

The E-banking Concept

According to Chaimaa et al. (2021), the emergence of advanced technologies has led to a highly interconnected and digitalised banking landscape, resulting in a paradigm shift in customer preferences and financial management practices. Consequently, most bank clients now prefer to access services electronically, choosing to do so at their convenience anytime and anywhere (Tsai & Su, 2021). Several terms are used interchangeably to describe e-banking, including online banking, digital banking, virtual banking, cyber banking, and internet banking (Ali et al., 2019). In simple terms, Drigă and Isac (2014) define e-banking as the delivery of banking services by financial institutions to clients through digital platforms, eliminating the need to visit a physical branch. Literature confirms that e-banking offers significant benefits to both banks and their customers, as it is relatively cost-effective, facilitates the prompt and secure exchange of important information, and enables the buying and selling of goods or services from any location at any time (Chaimaa et al., 2021). In the South African context, most banking services, such as account balance inquiries, loan applications, money transfers, payment processing, investment activities, and insurance-related transactions can now be conducted online. Thus, the act of accessing banking services digitally through an internet-connected device is referred to as e-banking. The current study aims to investigate the key drivers behind the surge in e-banking fraud occurring across digital banking platforms.

Prior literature (Chindara et al., 2025b) has identified opportunity, pressure, and technological advancement as contributing factors to the prevalence of e-banking fraud in developing countries such as South Africa. The findings of this study support the dictates of the Fraud Diamond Theory (FDT), particularly its two elements, opportunity and pressure, in explaining what drives cybercriminals to commit fraud. However, the FDT was



originally tailored to occupational fraud, and prior studies relied predominantly on quantitative approaches, which may have overlooked valuable insights obtainable through qualitative perspectives. Qualitative research, especially through in-depth interviews, enables participants to share richer and more nuanced information about the problem at hand. Accordingly, the present study seeks to address this gap by adopting a comprehensive qualitative methodological framework.

E-banking fraud

According to the South African Fraud Prevention Services (SAFPS, 2021), fraud is defined as any act involving the deliberate concealment, omission, or distortion of the truth to deceive another person or to obtain an unlawful or unfair advantage, resulting in financial, reputational, or legal harm to another party. Yusti et al. (2021) further note that fraud may be perpetrated intentionally by either an individual or a group seeking personal gain, while causing or potentially causing harm to others. Such acts violate established legal and ethical standards. Clearly, fraud stems from intentional conduct, wherein the perpetrator knowingly deceives another into believing something untrue. This deception typically results in loss or damage to the victim, while the perpetrator benefits personally. The term e-banking fraud is a generic term used to categorise a form of fraud, with emphasis on how and where it was perpetrated. Chindara (2024, p. 181) offers a precise definition, stating: “It is an intentional act by persons, individual or collective perpetrated with deception influenced by pressure from a need utilising any opportunity enabled by technological advancement to gain trust of the victim (bank customer, bank employee or bank system) which will potentially or effectively cause a direct or indirect loss (monetary or non-monetary) by the aide of an electronic device connected on internet”. Direct loss occurs when the victim loses money, property, or other valuables as a result of the fraudulent act. Indirect loss, on the other hand, may include additional consequences suffered due to the fraud, for instance, the loss of employment, friendships, trust, reputation, or even the onset of depression. Fraud therefore has far-reaching negative consequences, affecting individuals in their personal capacity, as well as businesses and nations more broadly. It is thus imperative to devise reliable and efficient frameworks to mitigate its prevalence. Equally, there is an urgent need to identify the underlying causes of fraud in order to inform the development of accurate and effective anti-fraud solutions.

Theoretical Framework

The Fraud Diamond Theory was adopted in the present study as it offers valuable insights into the possible causes of e-banking fraud prevalence within South African banking institutions. Proposed by Wolfe and Hermanson in 2004, the theory extends the earlier Fraud Triangle Theory developed by Cressey in the 1950s (Ruankaew, 2016). Wolfe and Hermanson (2004) argued that perceived pressure, opportunity, and rationalisation alone without the element of capability cannot result in a successful fraud attempt. Consequently, the FDT introduced capability as the fourth component. The theory posits that a fraudster must possess the requisite skills and ability to execute the fraud for it to succeed (Rustiarini et al., 2019).

Pressure is defined as any real or perceived force that drives an employee, at any level of the organisation, to commit fraud. Cressey (1953) described pressure as an unshareable problem or challenge. Extant literature



broadly concurs on two principal categories of pressure: financial and non-financial, with financial pressure being the most prevalent (Chindara et al., 2025; Mangala & Soni, 2023; Avortri & Agbanyo, 2021; Wolfe & Hermanson, 2004). Financial pressures stem from monetary needs and may include large expenses or personal debt resulting from unmet financial expectations or living beyond one's means (Jackson Albrecht et al., 2010). Notably, Albrecht et al., (2006) attributed 95% of organisational fraud to financial pressure. Within the banking sector, studies by Hollow (2014) and Chindara et al. (2025b) identified pressure as a primary driver of committing fraud. Accordingly, the present study hypothesises that pressure is one of the key drivers of e-banking fraud in South Africa.

Opportunity is another element identified by the FDT as contributing to occupational fraud within organisations (Wolfe & Hermanson, 2004). The literature supports the notion that weak systems, inadequate internal controls, and failures in organisational processes create opportunities for employees to exploit vulnerabilities and commit fraud (Ruankaew, 2016; Albrecht et al., 2006). Given that cyber criminals may actively seek such opportunities, it is imperative for management as agents of the organisation to implement robust internal controls and processes to deter fraudulent activity (Chindara, 2024). Accordingly, this study hypothesises that the opportunities for the prevalence of e-banking fraud created by digital banking platforms are contributing to the surge in fraud cases in South Africa.

Rationalisation, the third element, was originally introduced in Cressey's Fraud Triangle (1953). It refers to the justifications individuals use to legitimise fraudulent behaviour, allowing them to perceive their actions as acceptable or even necessary (Rustiarini et al., 2019). Rationalisation alleviates guilt, enabling the fraudster to maintain a sense of moral comfort (Murphy & Dacin, 2011). Therefore, the fraudster must be psychologically and mentally resilient to endure the stress associated with prolonged fraudulent behaviour (Rustiarini et al., 2019; Wolfe & Hermanson, 2004). Jackson et al. (2010) concluded that an individual cannot proceed with fraud unless they rationalise the act as ethically justifiable. Thus, the study hypothesises a positive relationship between the prevalence of e-banking fraud and the rationalisations employed by fraudsters, which are further facilitated by the anonymity afforded by digital banking platforms.

The fourth and newly added element in the FDT is capability, the fraudster's ability to skilfully and competently execute the fraud without obstruction and detection, often facilitated by their position within the organisation. Wolfe and Hermanson (2004) argued that an individual's role provides the capacity to exploit identified opportunities. Thus, even if a fraudster experiences pressure, spots the opportunities available and rationalises the act, they cannot successfully commit fraud without the capability to do so. The theory highlights factors such as organisational position, intelligence, confidence, and stress management as key sources of capability (Rustiarini et al., 2019). Therefore, this study hypothesises a positive relationship between the prevalence of e-banking fraud and the capacity of fraudsters, facilitated both by the nature of digital transactions and by their ability to devise complex attack tools.

The elements of the FDT offer valuable insights into the increasing incidence of fraud within organisations. The inclusion of the fourth element, capability in its multiplicity, makes the theory particularly effective in



identifying potential causes of fraud in the modern business environment. While Cressey's Fraud Triangle (1953) initiated the discourse on what drives employees to commit fraud, the FDT presents a more refined perspective, which is why it was adopted in the current study. However, these previous fraud theories primarily focused on occupational or organisational fraud committed within the organisation or employed alternative methodological approaches to data collection and analysis (Avortri & Agbanyo, 2021; Sham et al., 2023; Mangala & Soni, 2023). Additionally, Chindara et al. (2025a) examined similar themes; however, they were limited to the elements of the Fraud Triangle and the adoption of digital technologies as contributing factors. In contrast, this study aims to explore the causes of e-banking fraud in South African banks, focusing particularly on digital platforms and external fraudsters rather than internal bank employees. Additionally, prior studies employed quantitative methods, which may have constrained the depth of insight. Therefore, the current qualitative study is expected to yield richer understanding of the key drivers of e-banking fraud in South Africa, guided by Wolfe and Hermanson's (2004) FDT.

METHODOLOGY

The researchers adopted an interpretivist philosophy, motivated by the need to gain detailed insights from respondents to identify the key drivers behind the prevalence of e-banking fraud in South African banks. This choice aligns with the guidance of Kaushik and Walsh (2019), who note that the interpretivist approach is particularly suited to studies where researchers rely heavily on information provided by participants to form subjective interpretations of phenomena. Furthermore, an inductive approach was employed, as the study aims to generate rich, qualitative data through human interpretation, which serves as the primary source of research evidence (Collis & Hussey, 2003).

Sampling and Data Collection Process

The research population comprised both South African local banks and branches of foreign banks that are regulated and governed by the SARB, as listed on its official website as of 31 December 2020. According to Pandey and Pandey (2021), sample design can be categorised as either probabilistic or non-probabilistic. This study adopted a non-probabilistic sampling approach, whereby the sample was purposefully selected by the researcher based on criteria such as market share, the range of digital services offered, and geographical location, to yield the most meaningful results.

A sample of five banks was selected: three with Tier 1 capital exceeding US\$3 billion, and two from other local banks. To preserve the anonymity of the banks from which respondents were selected, pseudonyms were assigned: Bank A, Bank B, and Bank C for the major institutions, and Bank Y and Bank Z for the smaller ones. To ensure the depth and quality of insights, as well as the timely collection of research data, a purposive sample of 15 respondents was selected for interviews. The study employed a qualitative approach, with data collected through semi-structured online interviews. These interviews targeted senior risk professionals, whose perspectives were considered most relevant given their expertise within the risk fraternity and their direct exposure to the consequences of cybercrime, thereby minimising any possibility of selection bias. Pistrang and



Barker (2012) commend interviews as an effective method for collecting rich, nuanced data, offering in-depth insights and textured descriptions during qualitative inquiries.

Virtual interviews were scheduled and conducted using the Microsoft Teams platform, which supports video interviews. Appointments were arranged using contact details provided by the human resources or research departments of the respective banks. These video interviews closely resembled face-to-face interactions, allowing the researcher to observe body language and other non-verbal cues (Saarijärvi & Bratt, 2021). The method was chosen for its convenience and cost-effectiveness, as it eliminated the need for travel. Data collection was carried out over a four-month period, from May to August 2023. Interview transcripts were downloaded immediately after each session to prevent data loss, and each transcript was clearly labelled to avoid confusion. Additionally, each interview was recorded, and the audio files were saved in a dedicated folder on a USB flash drive, with appropriate naming conventions applied for easy reference.

Data Presentation and Analysis

Following the successful completion of all 15 interviews, the researchers commenced the data curation and cleaning process for each interview transcript. This step was essential, as it involved identifying and correcting any omissions or inaccurately transcribed words that the Microsoft Teams recording software may have failed to capture. Corrections were made using the audio recordings from the interviews, supplemented by notes taken by the researcher during each session. Once cleaned, the transcripts were uploaded into MAXQDA 24 software for thematic analysis. According to Lochmiller (2021), thematic analysis is a qualitative research method used to identify and examine patterns and themes within a dataset. It involves systematically organising and interpreting textual or visual data to uncover underlying meanings and gain deeper insight into the subject under investigation (Thompson, 2022).

Through this process, meaningful segments of data were identified and labelled, resulting in the generation of codes from the software-analysed content. The coding process aimed to capture key ideas (Kiger & Varpio, 2020) and concepts related to the drivers of e-banking fraud prevalence in South Africa. A like-for-like categorisation approach was applied, grouping similar codes to form initial themes. These themes reflected the core ideas and insights emerging from the data. Finally, in accordance with Thompson (2022), the codes were defined and analysed. The findings were presented using tables and charts, and selected direct quotations from participants were included to substantiate key concepts and interpretations.

Ethical Considerations

A pilot study was carried out in five Zimbabwean banks to evaluate the adequacy of the research instruments before the final interviews. Based on feedback from the pilot study, the interview questions were refined accordingly. Zimbabwean banks were selected for the pilot due to their close resemblance to South African banks, shaped by a shared colonial history. The legacy of a common coloniser has resulted in striking similarities between the banking sectors of the two countries. Furthermore, several Zimbabwean banks are branches of South African institutions, making the pilot study sample highly comparable to the main study population. Additionally, participants were assured that all data collected would remain anonymous and be



treated with strict confidentiality. They were also informed of their right to withdraw from the study at any point should they choose to do so. Nonetheless, respondents were encouraged to complete the interviews to enable the formulation of well-informed recommendations for the South African banking sector.

RESULTS

Table 1 summarises the key themes and drivers formulated from the data analysed using MAXQDA 24 software, along with the corresponding responses, which were examined both numerically and as percentages.

Table 1. Study Findings

Number	Theme	Driver	Agreeing		Disagreeing		Total Responses	
			NO:	%age	NO:	%age	NO:	%age
1	Connivance	Collusion between bank staff and cybercriminals leading to an information breach.	9	60%	6	40%	15	100%
2	Technological advancement	1. The rapid advancement and adoption of technology	15	100%	0	0%	15	100%
		2. Overdependence on e-banking platforms	10	67%	5	33%	15	100%
3	Inadequate Research	New products leveraging emerging technologies are often launched with limited, inadequate, or no prior research	12	80%	3	20%	15	100%
4	Pressure	1. Financial pressures: Rising levels of debt, increased reliance on loans, impulsive spending habits, and living beyond one's financial means continue to strain individual and institutional stability.	13	87%	2	13%	15	100%
		2. Non-financial pressures: External factors such as pandemics and widespread unemployment have disrupted ethical norms and societal values, thereby increasing the prevalence of e-banking incidents.	14	93%	1	7%	15	100%
5	Opportunity	The anonymity and complexity of e-banking transactions provide fertile ground for cybercriminals to launch attacks with little or no fear of apprehension.	15	100%	0	0%	15	100%
6	Rationalisation	1. Rationalising the reasons to commit fraud motivates cyber fraudsters to commit e-banking fraud in South Africa.	12	80%	3	20%	15	100%
		2. A rational fraudster capitalises on the remoteness of e-banking platforms to commit fraud.	14	93%	1	7%	15	100%
7	Human capital	1. Lack of forensic expertise and investigative skills	11	73%	4	27%	15	100%
		2. Insufficient employee education and training on emerging technologies	13	87%	2	13%	15	100%
		3. Limited capabilities in digital information extraction and data handling	12	80%	3	20%	15	100%



		4. Low client awareness and understanding of new technological innovations	15	100%	0	0%	15	100%
		5. Inadequate skills in investigating digital banking fraud	9	60%	6	40%	15	100%
8	Regulatory	1. Inadequate laws and regulations to combat fraud on digital platforms	9	60%	6	40%	15	100%
		2. A weak legal and regulatory environment	8	53%	7	47%	15	100%
9	Weaknesses in judicial follow-through.	1. Weakness within law enforcement agencies and the judicial system.	10	67%	5	33%	15	100%
		2. Prolonged delays in the finalisation of cases.	9	60%	6	40%	15	100%
		3. Lack of automation in judicial processes, resulting in inefficiencies and delays	9	60%	6	40%	15	100%
10	Governance and Compliance Weaknesses	1. Insufficient oversight by top management over systems and internal controls	8	53%	7	47%	15	100%
		2. Management override of established internal control mechanisms	4	27%	11	73%	15	100%
		3. Failure to adhere to documented policies and procedures during critical processes such as recruitment	3	20%	12	80%	15	100%
11	Financial	1. Budgetary constraints resulting from limited prioritization of e-banking fraud defenses	14	93%	1	7%	15	100%
		2. High costs associated with advanced technological software for fraud detection and prevention	12	80%	3	20%	15	100%
12	Operational and Institutional Limitations	Lack of appropriate tools and information-handling expertise within both banks and law enforcement agencies	11	73%	4	27%	15	100%
13	Scarcity of reliable information on fraud data	1. Limited availability of fraud-related data within the banking sector hampers effective risk assessment and response strategies	15	100%	0	0%	15	100%
		2. Deliberate concealment of fraud incidents by institutions seeking to protect their reputation and avoid further targeted attacks	14	93%	1	7%	15	100%
		3. Absence of a centralised fraud database in South Africa undermines coordinated efforts to detect, prevent, and investigate financial crimes	12	80%	3	20%	15	100%
14	Technological and Systemic Challenges	1. Lack of robust fraud mitigation systems to effectively combat e-banking fraud on digital platforms	13	87%	2	13%	15	100%
		2. Insufficient deployment of advanced technologies such as Artificial Intelligence (AI), Blockchain, and Machine Learning (ML) to alleviate the growing scourge of e-banking fraud	15	100%	0	0%	15	100%



		3. Use of compromised internet facilities by some clients, increasing vulnerability to cyberattacks	11	73%	4	27%	15	100%
		4. Inadequate data encryption, outdated software, and lack of regular system updates	12	80%	3	20%	15	100%
		5. Absence of an integrated ML-powered e-banking fraud risk management framework for deterrence, prevention, detection, and response	14	93%	1	7%	15	100%
		6. Inaccessibility of South Africa-tailored fraud risk management systems	8	53%	7	47%	15	100%
		7. Lack of customised fraud risk management frameworks designed specifically for South African banks	13	87%	2	13%	15	100%
15	Policy and Operational Gaps	1. South African banks have fraud policies in place; however, these policies require regular updates to remain aligned with the evolving business environment.	9	60%	6	40%	15	100%
		2. There is limited support from dedicated fraud units, including the absence of a 24-hour fraud customer care service, which hampers timely response and resolution.	10	67%	5	33%	15	100%
16	Receiving and logging of complaints	1. The current workflow is heavily reliant on manual procedures, resulting in inefficiencies and delays	14	93%	1	7%	15	100%
		2. There is a lack of automated, real-time fraud detection and reporting systems to ensure timely intervention and response	8	53%	7	47%	15	100%

Source: Own construct

DISCUSSION

Drivers in line with the FDT

The discussion of the findings begins by assessing whether the propositions of the FDT are satisfied in relation to the commission of e-banking fraud in South Africa. Opportunity, one of the core elements of the FDT, was subsequently identified as a key driver of e-banking fraud prevalence, as shown in item 5 of Table 1 above. The study found that the virtual environment creates opportunities for e-banking fraud, as clients can be easily deceived by fraudsters into divulging confidential account details. This is facilitated by the anonymity and complexity of digital banking transactions, which fraudsters exploit by leveraging advanced technologies to devise sophisticated and harmful fraud attacks. This conclusion is corroborated by Mangala and Soni (2023), as well as Chindara et al. (2025a), who likewise found that opportunity plays a pivotal role in facilitating the perpetration of fraud. It is therefore imperative that bank management and South African regulators remain attuned to these opportunities to identify and deploy the appropriate tools to counteract them effectively.



Secondly, item 4 of the study results presented in Table 1 indicates that pressure contributes significantly to the prevalence of e-banking fraud within the South African banking sector. The findings indicate that 87% and 93% of respondents believe that financial and non-financial pressures, respectively, within South African communities are driving the rise in e-banking fraud. This observation aligns with the FDT and suggests that much like occupational fraud, pressure can serve as a powerful motivator for cybercriminals to target banks and their customers, resulting in substantial and unprecedented losses across the sector.

This insight reinforces the work of Cressey (1953) and Wolfe and Hermanson (2004), who identified pressure as a fundamental component in the commission of fraudulent acts. Initiatives rooted in social responsibility, such as educating young people on entrepreneurship, providing start-up capital, and raising public awareness about the consequences of fraud, may help to alleviate these pressures within the South African economy. Therefore, banks and the South African government need to undertake social responsibility initiatives that empower communities, ultimately reducing the pressure of basic life needs and mitigating the scourge of e-banking fraud.

Furthermore, respondents highlighted that the secrecy inherent in digital banking platforms diminishes the probability of identification and apprehension, thereby emboldening fraudsters and facilitating the rationalisation of their actions, as reflected in item 6 of the results table above. Therefore, the hypothesis that rationalisation has a positive relationship with e-banking fraud in South Africa is supported. This finding aligns with Rustiarini et al. (2019) and Wolfe and Hermanson (2004), who argue that fraudsters must be resilient enough to withstand the psychological stress associated with fraudulent acts. In this regard, the confidence of not being detected, afforded by the anonymity of the digital environment, strengthens their persistence in perpetrating e-banking fraud. Consequently, banks and regulatory authorities must strengthen their anti-fraud awareness programmes to counter the powerful rationalisations that often stem from ignorance of the fact that individuals can indeed be apprehended if caught engaging in digital fraud.

Lastly, respondents agreed that advances in technology enable cybercriminals to develop highly effective attack tools. Respondent 4 from Bank Y stated, *“The ability to bypass all systems and controls is crucial for e-banking fraud to thrive. With the introduction of new technologies, the capacity of cybercriminals has been significantly altered. These advancements enable fraudsters to develop sophisticated attack tools that can easily circumvent existing controls designed to prevent and detect banking fraud. As such, we regard these technological developments as a double-edged sword, which we can utilise to strengthen our defences, but which can equally be exploited by fraudsters to launch seamless attacks.”* Hence, these complexities increase the capacity of fraudsters to perpetrate e-banking fraud within the South African Banking Sector (SABS), as illustrated in item 2 of Table 1. This finding aligns with Rustiarini et al. (2019), who emphasised that the capacity to exploit identified opportunities directly contributes to the success of fraudulent attacks. Accordingly, mitigating e-banking fraud in South Africa requires the deployment of advanced counter-technological tools designed to curtail cybercriminals’ capacity and ensure maximum protection.



In this regard, all four elements of the Fraud Diamond Theory-opportunity, pressure, rationalisation, and capability-were found to be pertinent in driving e-banking fraud within the SABS. Therefore, bank management, academia, regulators, and anti-fraud bodies can recommend effective e-banking fraud defences by drawing insights from these elements of the FDT.

Independent Drivers for e-banking fraud prevalent in South Africa

The study found that collusion between bank employees and cybercriminals is one of the key factors contributing to the rise in successful fraud attacks within South African banking institutions. As reflected in item 1 of Table 1, the assertion received support from 60% of the respondents. Thus, insiders provide customers' authentication details to criminals, who then use this confidential information to defraud the victims. Existing literature suggests that most successful fraud attacks involve some form of insider collaboration (SABRIC, 2018). Furthermore, overreliance on e-banking services was identified as an additional contributor to the surge in e-banking fraud within the South African banking sector. This finding aligns with prior literature, including SABRIC (2024), Tawde et al. (2024), and Basel (2024), all of which report a positive correlation between the increased adoption of digital banking platforms and the prevalence of banking fraud. In this regard, robust systems and controls must be embedded within the banking framework and constantly upgraded to ensure protection against technological advances, while also eliminating opportunities for collusion between internal staff and cybercriminals.

Most respondents, 12 out of 15 (80%), allege that most digital banking technologies are being adopted hastily, either to gain a competitive edge or to safeguard against emerging threats. This rapid adoption often occurs without sufficient research into the potential drawbacks of these products or services. Consequently, this has led to a rise in e-banking fraud, as unscrupulous cybercriminals actively seek vulnerabilities within these systems, products, or services to exploit them before institutions become aware of the gaps in their technological tools or solutions. South African banks must establish robust research and development departments tasked with thoroughly interrogating each product or service prior to adoption. This would enable them to identify potential weaknesses or risks associated with each offering before cybercriminals do.

Respondents also highlighted deficiencies in effective real-time digital banking fraud mitigation tools, forensic expertise, investigative capabilities, and digital information extraction and handling skills as key contributors to the high prevalence of e-banking fraud in the South African banking sector. This finding aligns with Phiri et al. (2024) and Pillay et al. (2023), who noted that investigators within both law enforcement agencies and banks in South Africa lack the technological tools and specialist skills required to address digital banking cases effectively. Furthermore, respondents observed that experts in these fields are migrating to developed economies in search of better opportunities, where they are more generously compensated. This claim is also supported by Pillay et al. (2023). As such, banks and regulatory authorities must reconsider and enhance the remuneration packages for professionals in this domain in order to retain critical talent.

In addition, all respondents (100%) reported deficiencies in technological education, training, and awareness among both bank customers and employees. This is corroborated by extant literature, which



emphasises that educating and training both bank staff and customers on new technologies prior to their implementation is a critical measure (Dzomira, 2016; Barker, 2020; SABRIC, 2024; Phiri et al., 2024). Such proactive engagement enables clients and employees to be sensitised to the potential risks associated with the use of specific e-banking tools and services. Accordingly, banks must conduct regular technological training and educational workshops for both clients and employees, and South African policy should mandate these initiatives to ensure their comprehensive implementation.

Commendably, there are fewer challenges relating to governance and compliance weaknesses in the South African banking sector. This is evidenced by the fact that 80% of respondents indicated that bank management adheres to documented policies and procedures during critical processes such as recruitment, while 73% affirmed that management does not override established internal control mechanisms. However, 53% of respondents believed that there is insufficient oversight by top management over systems and internal controls within South African banks, which may be contributing to the high prevalence of e-banking fraud in the sector.

Respondent 3 from Bank A remarked, *“There is a pressing need for top management to exercise thorough oversight over all system-related matters, while strictly adhering to internal controls and established procedures. If we are sincere in our desire to combat the scourge of bank fraud, this is essential. This will close existing gaps and strengthen our controls. For example, conducting proper background checks during recruitment can prevent banks from hiring individuals with a history of fraud, who may later collude with external criminals to defraud the bank or its customers.”* This view is supported by Fernandes and Dias (2024), who emphasise the importance of implementing and adhering to robust internal controls, maintaining clear segregation of duties, and ensuring continuous monitoring by senior management. The current study recommends that senior management within South African banks continue to uphold sound governance practices and comply with relevant procedures, laws, and regulations. Furthermore, the study encourages senior management to exercise diligent oversight of advanced technological systems and controls to ensure their integrity and effectiveness.

Additionally, the inadequacy of laws and regulations to effectively combat fraud on digital platforms was cited as a significant hindrance to curbing e-banking fraud in South Africa. This assertion is supported by around 57% of the respondents. Additionally, respondent 1 from Bank C emphasised, *“The South African government has been consistent in its efforts to upgrade regulations aimed at addressing such fraud since the early 2000s. This has led to the establishment of several anti-fraud bodies, such as SAFPS, SABRIC, and CSIRT, which have played a pivotal role in safeguarding banks, customers, and their funds from these audacious fraudsters. Their interventions have helped protect countless South Africans and prevented billions in losses. However, there remains a discernible gap between existing regulations and the evolving methods of e-banking fraud, resulting in low conviction rates. Many cyber fraudsters are acquitted due to shortcomings within the judicial system, even when compelling evidence is presented. I therefore recommend that these regulations be revised through broad consultation with various stakeholders, ensuring they are both resilient and holistic.”* The issue of regulatory gaps within South African law is further supported by Pillay et al. (2023),



who emphasised a fundamental weakness in the Cybercrime and Cybersecurity Bill. Specifically, the study concluded that existing legislation fails to provide a comprehensive account of the technological dimensions of cybercrime, including attack mechanisms and hacking vulnerabilities. Moreover, weaknesses in judicial process flows require urgent attention, a concern underscored by 67% of the respondents. These deficiencies were further corroborated by Pillay et al. (2023), who observed that such shortcomings contribute to delays in the finalisation of e-banking fraud cases. In light of this, and as proposed by Respondent 1 from Bank C, there is an urgent need for collaborative efforts among banks, regulators, customers, network providers, government agencies, law enforcement bodies, the judiciary, academia, and independent anti-fraud organisations. Such cooperation is essential for the development of robust and inclusive laws and regulations that address the full spectrum of digital banking fraud. Additionally, the automation of processes within judicial services could play a significant role in mitigating these weaknesses across government institutions.

Budgetary constraints and the high cost of e-banking fraud defences were identified as key obstacles in combating e-banking fraud within South African banks, as indicated in item 11 of Table 1. Respondents (93%) indicated that senior management is not prioritising fraud mitigation measures during budget formulation. Additionally, the absence of well-defined, locally tailored fraud defences in the South African market was noted, thereby leaving banks with little choice but to adopt pre-existing solutions designed for developed countries often at considerable expense. This assertion concurs with Akinbowale et al. (2024), who noted that management should actively pursue the development of South African-specific e-banking fraud defences to help reduce the incidence of fraud within the sector. It is therefore imperative that senior management prioritise the fight against cyber fraud by allocating adequate funding and prioritising locally developed anti-fraud countermeasures to address the issue.

The study also found that, although South African banks have been consistent and vigilant in deploying contemporary technological solutions to curb banking fraud, there remain significant inadequacies in systems designed to combat e-banking fraud. However, major deficiencies identified by respondents include: the lack of robust fraud mitigation systems capable of effectively addressing e-banking fraud on digital platforms; insufficient deployment of advanced technologies such as AI, Blockchain, and ML to counter the growing scourge of e-banking fraud; inadequate data encryption; outdated software; and a lack of regular system updates. Additionally, all (100%) of the respondents noted the absence of an integrated ML-powered e-banking fraud risk management framework for deterrence, prevention, detection, and response. This finding is supported by Phiri et al. (2024), who also observed a continued shortage of effective e-banking fraud defences in South Africa. Thus, as recommended by the respondents, banks should adopt emerging technologies, particularly those leveraging ML with robust anomaly detection capabilities, which may prove effective in both preventing and detecting fraud.

Moreover, the scarcity of fraud-related data within the SABS emerged as a significant challenge identified by all the respondents (100%). Representatives from Banks X and Y shared the following insights:



Bank Y, Respondent 2, stated: *“There is a severe drought of fraud statistics in the South African banking sector, which is significantly hindering the adoption of emerging technologies such as supervised machine learning models. These models require substantial data for training in order to effectively detect and mitigate fraudulent activity. Banks are reluctant to share fraud-related information, primarily to safeguard their reputations. I would, however, advocate for the implementation of stringent regulations by the relevant authorities to compel all banks to report any incidents of fraud. This could be facilitated electronically through the creation of a centralised fraud database encompassing all banks operating in South Africa, where every attack experienced is recorded. Such a system would help accumulate the necessary data to combat the scourge of e-banking fraud.”*

Bank Z, Respondent 1, commented: *“Banks are reluctant to release fraud statistics, concerned that such disclosure might invite more targeted attacks from criminals and expose their vulnerabilities to the wider public. In today’s highly competitive environment, reputation is crucial for retaining clients. Revealing instances of fraud could be akin to self-sabotage, as customers may discreetly shift to institutions they regard as more secure. As a result, there is a significant shortage of digital banking fraud data within the sector. This absence of reliable information hampers efforts to combat fraud, leaving banks without the necessary data to test and validate their detection models on digital platforms.”*

It is evident that banks are hesitant to disclose statistics relating to fraud encountered in their daily operations. To address this issue, South African regulatory authorities must introduce robust regulations mandating full disclosure of all fraud incidents by banks (Bank Z, Respondent 2). Furthermore, under the guidance of these authorities, the banking sector should establish a centralised fraud database, updated in real time, to record all incidents reported by financial institutions. This central repository of fraud data would help alleviate the current information drought that is undermining efforts to combat fraud, particularly those reliant on historical data for predictive modelling.

Moreover, respondents highlighted certain policy and operational shortcomings within South African banks, as indicated in item 15 of the results table. While it was acknowledged that banks do have robust policies and procedures in place to prevent fraud, these frameworks are not consistently updated to reflect the evolving business environment. Dzomira (2017) supports the notion of regularly reviewing and revising such policies to align with the dynamic operational landscape, thereby preventing procedural gaps that could be exploited by criminals to defraud financial institutions.

In addition, 67% of respondents reported limited support from dedicated fraud units, notably the absence of a 24-hour fraud customer care service, which significantly impedes the timely response and resolution of cases. The findings further confirm that although South African banks are increasingly adopting technological solutions, their current fraud detection workflows remain heavily reliant on manual processes. This dependence results in inefficiencies and delays, particularly in responding to incidents outside standard operating hours. The lack of automated, real-time fraud detection and reporting systems presents a critical gap in the effectiveness of fraud detection and investigation. Fraudulent activities occurring during off-peak hours



often go unreviewed for extended periods, potentially exacerbating financial losses for both banks and their customers due to cyberattacks. Therefore, banks need to invest in advanced technological solutions capable of detecting fraud in real time. Additionally, establishing round-the-clock fraud review services would significantly enhance response times and improve the overall resilience of the banking sector against fraudulent threats.

LIMITATIONS

The study recognised some of its limitations, which include being cross-sectional and the sample being drawn solely from South African banks, which may complicate the generalisation of the findings to other developing countries. Therefore, further studies on the same topic might be conducted over a longer period and could produce different or more informed positions regarding the key drivers of e-banking fraud prevalent in South Africa. In addition, studies drawing on samples from multiple countries could provide deeper insights into the factors driving the prevalence of e-banking fraud, despite banks deploying various defences to mitigate it. Furthermore, the researchers acknowledge the possibility of respondent selection bias arising from the purposive non-probability sampling technique employed in the present study. Consequently, further research on this topic should be undertaken utilising alternative sampling techniques.

CONCLUSION

This study examined the principal drivers of e-banking fraud in South African banks through qualitative methods, notably virtual interviews with 15 participants drawn from both local and branches of international institutions. The analysis was conducted using MAXQDA 24, and the study was theoretically guided by the FDT to formulate assumptions regarding the key drivers of e-banking fraud prevalence in South Africa. The findings confirmed that opportunity, pressure, rationalisation, and capability collectively underpin the incidence of e-banking fraud. The salient drivers identified include rapid technological adoption, collusion between employees and cybercriminals, insufficient research, limited forensic expertise, weak regulatory frameworks, judicial inefficiencies, poor governance, scarcity of reliable data, systemic challenges, and reliance on manual complaint handling. The study concluded that bank management and other stakeholders may utilise these findings and recommendations to develop contemporary control mechanisms, anchored in advanced technologies such as ML and Blockchain, in order to mitigate e-banking fraud within the South African banking sector. Such measures are essential for safeguarding depositors' funds, ensuring accurate financial stewardship, and upholding ethical accountability to the public. Accordingly, the study contributes both practical and theoretical insights, recommending, among other solutions, the deployment of machine-learning systems for real-time fraud detection.

Conflict of interests: The authors declare no conflict of interest.



Authors' contributions: Conceptualization, T.M.C.; methodology, T.M.C.; software, T.M.C.; validation, T.M.C.; formal analysis, T.M.C.; investigation, T.M.C.; resources, T.M.C.; data curation, T.M.C.; writing-original draft preparation, T.M.C.; writing-review and editing, E.E.; visualization, T.M.C.; supervision, E.E. All authors have read and agreed to the published version of the manuscript.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors did not use Generative AI or AI-assisted tools to create or alter images in the manuscript.

Ethical Considerations and Institutional Review Board Statement:

All research processes and writing adhered to established ethical standards. In addition, an ethical clearance certificate was issued by the relevant authorities.

Consent-to-participate: Consent from the respondents was obtained in written form.

Data availability statement: All data supporting the research findings are available upon request from the corresponding author.

References

- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, 31(1), 201–225. <https://doi.org/10.1108/JFC-02-2023-0025>
- Albrecht, W. S., Hill, N. C., & Albrecht, C. C. (2006). The ethics development model applied to declining ethics in accounting. *Australian Accounting Review*, 16(38), 30–40. <https://doi.org/10.1111/j.1835-2561.2006.tb00323.x>
- Ali, M. A., Hussin, N., & Abed, I. A. (2019). E-banking fraud detection: A short review. *International Journal of Innovation, Creativity and Change*, 6(8), 67–87
- Alisher, K. (2023). Accelerating Growth: The Impact of Digital Transformation on Banks' performance. *EPRA International Journal of Economics, Business and Management Studies (EBMS)*, 10(8), 8–11
- Asmah, A. E., Atuilik, W. A., & Ofori, D. (2020). Antecedents and consequences of staff related fraud in the Ghanaian banking industry. *Journal of Financial Crime*, 27(1), 188–201. <https://doi.org/10.1108/JFC-03-2019-0034>
- Avortri, C., & Agbanyo, R. (2021). Determinants of management fraud in the banking sector of Ghana: the perspective of the diamond fraud theory. *Journal of Financial Crime*, 28(1), 142–155. <https://doi.org/10.1108/JFC-06-2020-0102>
- Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management*, 51(1), 1–10. <https://doi.org/10.4102/sajbm.v51i1.1941>
- Basel Committee on Banking Supervision. (2024, May). *Digitalisation of finance*. Bank for International Settlements. Available at: <https://www.bis.org/bcbs/publ/d558.pdf> (Accessed on February, 12 2026)
- Chaimaa, B., Najib, E., & Rachid, H. (2021). E-banking overview: concepts, challenges and solutions. *Wireless Personal Communications*, 117(2), 1059–1078. <https://doi.org/10.1007/s11277-020-07911-0>
- Chindara, T. M. (2024). A framework for using machine learning to combat fraud in the South African banking sector (Doctoral dissertation). University of Johannesburg. Available at: <https://ujcontent.uj.ac.za/esploro/outputs/doctoral/A-framework-for-using-machine-learning/9955205907691> (Accessed on February 10, 2026)



- Chindara, T. M., Smith, J. R., & Leke, C. A. (2025a). Examining the nature and prevalence of e-banking fraud: a qualitative analysis of banks in South Africa. *Access to science, business, innovation in the digital economy*, ACCESS Press, 6(4), 303–318. [https://doi.org/10.46656/access.2025.6.2\(4\)](https://doi.org/10.46656/access.2025.6.2(4))
- Chindara, T. M., Smith, R. J., & Leke, C. A. (2025b). Examining the key drivers of electronic banking fraud prevalence in the South African banking sector. *Cogent business & management*, 12(1). <https://doi.org/10.1080/23311975.2025.2508366>
- Collis, J., & Hussey, R. (2003). *Business research: A practical guide for undergraduate and postgraduate students* (2nd ed.). New York: Palgrave Macmillan. ISBN: 978-0-230-30183-2
- Cressey, D. R. (1953). *Other people's money; a study of the social psychology of embezzlement*. Free Press
- Drigă, I., & Isac, C. (2014). E-banking services—features, challenges and benefits. *Annals of the University of Petrosani. Economics*, 14(1), 49–58
- Dube, S.C. (2018). Digital banks: game-changers in South Africa's banking industry? available at: <https://www.competition.org.za/ccred-blog-competition-review/category/Shingie+Chisoro+Dube> (Accessed on February 11, 2026)
- Dzomira, S. (2016). Financial consumer protection: internet banking fraud awareness by the banking sector. *Banks & bank systems*, 11(4), 127–134. [https://doi.org/10.21511/bbs.11\(4-1\).2016.03](https://doi.org/10.21511/bbs.11(4-1).2016.03)
- Dzomira, S. (2017). Internet banking fraud alertness in the banking sector: South Africa. *Banks & bank systems*, 12(1), 143–151. [https://doi.org/10.21511/bbs.12\(1-1\).2017.07](https://doi.org/10.21511/bbs.12(1-1).2017.07)
- Fernandes, T., & Dias, W. (2024). The effectiveness of internal controls in preventing fraud in banks. *Journal of Emerging Technologies and Innovative Research*, 11(9), 280–289
- Gupta, R., Gupta, S., & Ajekwe, C. C. M. (2023). Electronic Banking Frauds: The Case of India. In A. Rafay (Ed.), *Theory and Practice of Illegitimate Finance* (pp. 166–183). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-1190-5.ch009>
- Hollow, M. (2014). Money, morals and motives: an exploratory study into why bank managers and employees commit fraud at work. *Journal of Financial Crime*, 21(2), 174–190. <https://doi.org/10.1108/JFC-02-2013-0010>
- IT-Online (2022). Fraud surges as digital transactions dominate worldwide. Available at: <https://it-online.co.za/2022/12/06/fraud-surges-as-digital-transactions-dominate-worldwide/> (Accessed on February 4, 2026)
- Jackson, K., Holland, D., Albrecht, C., & Woolstenhulme, D. (2010). Fraud isn't just for big business: Understanding the drivers, consequences, and prevention of fraud in small business. *Journal of International Management Studies*, 5(1), 160–164
- Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social sciences*, 8(9), 255. <https://doi.org/10.3390/socsci8090255>
- Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical teacher*, 42(8), 846–854. DOI: 10.1080/0142159X.2020.1755030
- Laxman, V., Ramesh, N., Prakash, S. K. J., & Aluvala, R. (2024). Emerging threats in digital payment and financial crime: A bibliometric review. *Journal of Digital Economy*, 3, 205–222. <https://doi.org/10.1016/j.jdec.2025.04.002>
- Lee, S. (2025). *The evolution of bank fraud*. Number Analytics. <https://www.numberanalytics.com/blog/evolution-of-bank-fraud> (Accessed on: February 05, 2026)
- LexisNexis Risk Solutions. (2022, October 20). *Digital payment fraud in high growth markets study finds 90% of respondents experienced an increase in online fraud over past 12 months*. LexisNexis Risk Solutions. <https://risk.lexisnexis.com/about-us/press-room/press-release/20221020-fraud-in-emerging-markets-study> (Accessed on February 11, 2026)
- Lochmiller, C. R. (2021). Conducting thematic analysis with qualitative data. *The qualitative report*, 26(6), 2029–2044. <https://doi.org/10.46743/2160-3715/2021.5008>
- Malinka, K., Hujnak, O., Hanacek, P., & Hellebrandt, L. (2022). E-banking security study-10 years later. *IEEE Access*, 10, 16681–16699. <https://doi.org/10.1109/ACCESS.2022.3149475>
- Mangala, D., & Soni, L. (2023). A systematic literature review on frauds in banking sector. *Journal of Financial Crime*, 30(1), 285–301. <https://doi.org/10.1108/JFC-12-2021-0263>



- Mthimkhulu, A. (2024, November 5). *SABRIC report: Financial crime led to over R3bn loss in 2023 – what to know*. The South African. Available at: <https://www.thesouthafrican.com/news/sabrics-report-financial-crime-led-to-over-r3bn-loss-in-2023-what-to-know> (Accessed on February 5, 2026)
- Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: understanding and preventing fraud in organisations. *Journal of Business Ethics*, 101(4), 601–618. <https://doi.org/10.1007/s10551-011-0741-0>
- Nel, J., & Boshoff, C. (2021). Traditional-bank customers' digital-only bank resistance: evidence from South Africa. *International Journal of Bank Marketing*, 39(3), 429–454. <https://doi.org/10.1108/IJBM-07-2020-0380>
- Pandey, P., & Pandey, M. M. (2021). Research methodology tools and techniques. Bridge Center
- Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, 26(1), a1763, <https://doi.org/10.4102/sajim.v26i1.1763>
- Pillay, P., Ntuli, P. N., & Ehiane, S. O. (2023). Exploring the prevalence of cybercrime in the banking industry in KwaZulu-Natal, South Africa. *International Journal of Membrane Science and Technology*, 10(1), 1763–1775. <https://doi.org/10.15379/ijmst.v10i1.3283>
- Pistrang, N., & Barker, C. (2012). Varieties of qualitative research: A pragmatic approach to selecting methods. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 5–18). American Psychological Association. <https://doi.org/10.1037/13620-001>
- Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in accounting education*, 23(4), 521–533. <https://doi.org/10.2308/iace.2008.23.4.521>
- Ruankaew, T. (2016). Beyond the fraud diamond. *International Journal of Business Management and Economic Research*, 7(1), 474–476
- Rustiarini, N. W., Sutrisno, T., Nurkholis, N., & Andayani, W. (2019). Why people commit public procurement fraud? The fraud diamond view. *Journal of public procurement*, 19(4), 345–362. <https://doi.org/10.1108/JOPP-02-2019-0012>
- Saarijärvi, M., & Bratt, E. L. (2021). When face-to-face interviews are not possible: tips and tricks for video, telephone, online chat, and email interviews in qualitative research. *European Journal of Cardiovascular Nursing*, 20(4), 392–396. <https://doi.org/10.1093/eurjcn/zvab038>
- Sham, A. M., Muhammad, K., Ghani, E. K., & Sukmadilaga, C. (2023). Determinants of employee fraud in workplace: a fraud triangle perspective. *Economic Affairs*, 16(2), 1015–1025. <https://doi.org/10.46852/0424-2513.2.2023.5>
- Shetty, M. (2024). *Beware...800 Online Financial Frauds a Day*. *Times of India*. Available at: <https://timesofindia.indiatimes.com/city/mumbai/800-online-financial-frauds-a-day/articleshow/111242243.cms> (Accessed on: February 2, 2026)
- Shrier, D.L. (2022). Digital financial services. In: Shrier, D & A. Pentland (Eds.) *Global Fintech: Financial Innovation in the Connected World*, 73–90. <https://doi.org/10.7551/mitpress/13673.003.0008>
- Sijan, M. A. H., Shahoriar, A., Salimullah, M., Islam, A. S., & Khan, R. H. (2022). A review on e-banking security in Bangladesh: An empirical study. In *Proceedings of the 2nd international conference on computing advancements (ICCA '22)*. Association for Computing Machinery, New York, NY, USA, pp. 330-336. <https://doi.org/10.1145/3542954.3543002>
- Silva, A. J., & Dias, R. (2023). The role of financial status, attitudes, behaviours and knowledge for overall well-being in Portugal: the mediating role of financial well-being. *International Journal of Organisational Analysis*, 31(7), 3668–3685. <https://doi.org/10.1108/IJOA-08-2022-3385>
- South African Banking Risk Information Centre (SABRIC) (2018), “Digital banking crime statistics”. Available online at: <https://www.sabrics.co.za/wp-content/uploads/2024/11/SABRIC-Annual-Crime-Stats-2018-1.pdf> (Accessed on February 10, 2026)
- South African Banking Risk Information Centre (SABRIC). (2024, October 21). *SABRIC reports significant increase in financial crime losses for 2023*. Banking Association South Africa. Available at: <https://www.banking.org.za/news/sabrics-reports-significant-increase-in-financial-crime-losses-for-2023/> (Accessed on February 5, 2026)



- South African Banking Risk Information Centre. (2021). Annual crime statistics. <https://www.sabric.co.za/wp-content/uploads/2024/11/SABRIC-Annual-Crime-Stats-2021.pdf> (Accessed on February 6, 2026)
- Tawde, S.D., Arora, S., Thakur, Y.S. (2024). Online Payment Fraud Detection for Big Data. In: Devismes, S., Mandal, P.S., Saradhi, V.V., Prasad, B., Molla, A.R., Sharma, G. (eds) Distributed Computing and Intelligent Technology. ICDCIT 2024. Lecture Notes in Computer Science, vol 14501. Springer, Cham. https://doi.org/10.1007/978-3-031-50583-6_22
- Thompson, J. (2022). A Guide to Abductive Thematic Analysis. *The Qualitative Report*, 27(5), 1410–1421. <https://doi.org/10.46743/2160-3715/2022.5340>
- Tsai, C. H., & Su, P. C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information systems and e-business management*, 19(1), 77–105. <https://doi.org/10.1007/s10257-020-00481-5>
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42
- Yusti, M., Triyadi, T., & Ramadhan, D. (2021). Analysis of the Root Causes of Fraud Using Risk Causal and Fraud Diamond Matrix: A Case Study on Retail Financing Company. *Asia Pacific Fraud Journal*, 6(1), 159-170. <https://doi.org/10.21532/apfjournal.v6i1.202>

About the authors

Tawona Matrokisi CHINDARA,

Postdoctoral Fellow at Unisa, PhD in Accounting, College of Accounting Sciences, Department of Auditing,

Research interests: digital transformation and security, innovation, artificial Intelligence specialising in machine learning and fraud risk management.

ORCID ID: 0000-0001-5900-3773

Ebenezer ESENOGHO

(Senior Member, IEEE) received the Diploma and B.Eng. degrees (Hons.) in computer engineering, and the M.Eng. degree in telecoms engineering from the University of Benin, and the Ph.D. degree in electronics from the Center of Radio Access and Rural Technology (CRART), University of KwaZulu-Natal, Center of Excellence.

Research interests: fifth generation (5G) wireless networks, cognitive radio networks, network security/cybersecurity, smart grid networks, the IoT/IoE, SDN/SDR, wireless sensor networks, artificial intelligence/machine learning, big data, and mobile/cloud computing.

ORCID ID: 0000-0002-5328-1497

This work is licensed under the Creative Commons Attribution International License (CC BY)